UNCLASSIFIED

Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions | Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

In Camera Examination Summary: CSIS SITE Representative #1, CSIS SITE Representative #2, Ryan Macdonald, Robin Wettlaufer, Greg O'Hayon

Commission Counsel examined current and former representatives of the Security and Intelligence Threats to Elections Task Force ("**SITE TF**" or "**SITE**") during *in camera* hearings held in July and August 2024. Counsel for the Attorney General of Canada appeared on behalf of the Government of Canada and had the opportunity to examine the witness. The hearing was held in the absence of the public and other Participants. This summary discloses the evidence that, in the opinion of the Commissioner, would not be injurious to critical interests of Canada or its allies, national defence or national security.

Notes to Reader:

- Commission Counsel have provided explanatory notes in square brackets to assist the reader.

1. Examination by Commission Counsel

[1] The witnesses confirmed the accuracy of the summary of their panel interview and adopted its content as part of their evidence before the Commission.

1.1 Witnesses

[2] Ryan Macdonald was the Communications Security Establishment ("**CSE**") Representative on the SITE TF from May 2022 to May 2024. His role during that time was Director within an operational branch. Mr. Macdonald was the Chair of the SITE TF from May 2022 to November 2022.

[3] CSIS SITE Representative #1 is the Canadian Security Intelligence Service ("**CSIS**") representative and Chair of the SITE TF. They assumed this role in August 2023, succeeding CSIS SITE Representative #2. CSIS SITE Representative #1 also currently serves as Deputy Director General of CSIS' Policy and Strategic Partnerships Branch.

[4] CSIS SITE Representative #2 was the CSIS representative and Chair of the SITE TF from November 2022 to August 2023 and held a role in CSIS' Intelligence Assessment Branch during that time.

[5] Robin Wettlaufer is the Global Affairs Canada ("**GAC**") representative on the SITE TF. She assumed this role in September 2022. She also serves as Director of the Centre for International Digital Policy, which houses the Rapid Response Mechanism (RRM) [RRM Canada is also the Chair of the G7 RRM and serves as its permanent secretariat].

[6] Greg O'Hayon is the Royal Canadian Mounted Police ("**RCMP**") representative on the SITE TF. He assumed this role in March 2023. He also serves as the RCMP's Director General, Federal Policing Security Intelligence (previously Federal Policing Strategic Intelligence), within Federal Policing Intelligence and International Policing.

1.2 Current Threat Landscape: actors and methodologies

[7] Commission Counsel referred the witnesses to *SITE Threat Assessment of Foreign Interference Threats to Canadian Democratic Institutions* ("**SITE threat assessment**") from February 2024, and asked if threat assessments are produced on a regular schedule and, if so, what the timing would be.[1]

[8] CSIS SITE Representative #1 explained that the SITE threat assessment from February 2024 was produced ahead of the baseline threat assessment prepared for the March 4, 2024 by-election in the electoral district of Durham. The SITE TF has no particular schedule for producing general threat assessments and updates. CSIS SITE Representative #1 indicated that the current threat landscape was generally consistent with SITE's previous threat assessment dated June 2023[2]. However, in the February

[1] CAN037690.
[2] CAN040229.

2024 threat assessment, SITE TF added information about the key methodologies used by foreign states to help inform decision makers about how to respond to FI. CSIS SITE Representative #1 confirmed that all SITE members contribute to the production, updating, and revision of SITE TF's threat assessments, which end up becoming "corporate documents".

[9] In response to further questions from Commission counsel, Ms. Wettlaufer confirmed that RRM Canada does not do baseline monitoring of the domestic online environment except during general and by-elections. However, Ms. Wettlaufer confirmed that, if RRM Canada does learn something from international partners or they come across something as part of their work, they do share it with the SITE team.

[10] CSIS SITE Representative #1 then provided an overview of the current threat landscape. The PRC is the most active state actor engaging in traditional election interference [involving people and communities, as opposed to malicious cyber activities], followed by India, and to a lesser extent, Pakistan. One of the ways these state actors, particularly the PRC, conduct their FI is to rely on members of diaspora communities to conduct their FI activities in Canada. China's FI activities also rely on the existing networks developed by their Embassies and Consulates and, to a certain extent, on their intelligence services. Further, SITE has observed efforts from China and India to conduct FI activities in Canada by way of financing candidates. CSIS SITE Representative #1 described the PRC as continuing to have, even now, with the increased scrutiny, the capacity and the intent to engage in electoral FI against Canada through its FI networks. CSIS SITE Representative #1 added that SITE is concerned about alleged PRC interference in provincial, territorial, and Indigenous governments.

[11] Russia does not work within the system and instead works against it, with the aim to break it. CSIS SITE Representative #1 testified that Russia is attacking democracy at its core through mis- and disinformation campaigns and, increasingly, through generative-**artificial intelligence ("AI") [AI capable of generating text, images and videos]**. CSIS SITE Representative #1 emphasized that generative-AI is a concern for the SITE TF. Recently, the Panel of Five was briefed on these issues.

[12] The SITE TF is also paying close attention to Russia's mis- and disinformation campaigns aimed at interfering with recent international elections. CSIS SITE Representative #1 explained that Russia has made real efforts during recent elections, particularly in Europe (*e.g.*, France, UK), which have demonstrated its capacity to interfere in elections and that its efforts can have an impact in specific countries. He testified that we should ask ourselves both whether Canada might be the target of similar efforts and how Canada can prepare itself to successfully resist them. In response to a question from the Commissioner about whether Russia's interest and capabilities had changed since the 44th Canadian General Election ("**GE44**"), CSIS SITE Representative #1 explained that Russia currently is focused on the war in Ukraine and this drives much of the country's current disinformation efforts. Russia's capacity for mis-and disinformation in countries like Moldova and Slovakia has increased and this has borne fruit. These successes may serve to increase the efficiency of Russian interference campaigns and lead to wider efforts.

[13] Mr. Macdonald noted one additional change since the 43rd Canadian General Election ("**GE43**") and GE44, which is reflected in the threat assessment, which is the increased view of how generative-AI is impacting the information space, including the production of deepfake videos or imagery. CSE provided this information for the February 2024 SITE threat assessment, and the Canadian Centre for Cyber Security (CCCS) has also produced reports on the increase of cyber threats that have been observed worldwide in and around elections[3]. As part of those observations, CSE has seen a trend where there is more synthetic content (*e.g.*, manipulated or fabricated videos, audios, imagery) being put online in and around elections. AI now makes the creation and propagation of such content for mis- and disinformation purposes faster and easier. Doing the threat assessment allows SITE to think through how it would deal with new types of vectors for FI, such as this.

[14] Ms. Wettlaufer added that the advent of generative-AI has led to a proliferation of threat actors and lowered the barrier to entry for information manipulation. It is now easier for

[3] Mr. Macdonald referred the Commissioner to the Canadian Centre for Cyber Security 2023 Update on *Cyber Threats to Canada's Democratic Process* (public document).

individuals, countries, and organisations to conduct inauthentic coordinated disinformation campaigns. Ms. Wettlaufer said there has also been a proliferation of social media platforms. It is no longer enough to be monitoring the standard US-based platforms (Meta, X, etc.). There is a large and growing number of platforms, including ones based in China, in Belarus, and elsewhere. She agreed with the Commissioner that RRM Canada does not generally have API access to such platforms, and that it is therefore more labour intensive for RRM Canada to collect data from some of these new platforms because the unit is not able to use mass data scraping and analytical tools. As a result, much more manual monitoring and analysis is needed.

[15] CSIS SITE Representative #1 added that both China and Russia have the capacity to use generative-AI and may use it to conduct FI activities against Canada.

[16] Mr. Macdonald explained that SITE members have been actively reflecting on ways to detect and respond to the growing trend of influence campaigns that leverage generative-AI, and continue to do so, using table top exercises and looking at how the community can respond. Detecting online manipulation of content by foreign states can be difficult at times, as is determining the authenticity of content shared on social media, though he noted that SITE can rely on the media and other sources to do that as well. Over the past couple of years, the SITE TF agencies have received examples of suspected deepfake videos or audios and have used different techniques to determine their authenticity. The SITE TF is also working closely with partners within the Five Eyes.

[17] CSIS SITE Representative #1 added that SITE works to pool the tactical expertise of different departments with the aim of analyzing deep fakes and informing the government about the extent of that particular threat. The SITE TF will be conducting its own table top exercises in the fall. SITE members, with the help of various experts within their departments, will provide scenarios for the purpose of developing a proper response (attribution, assessment of legitimacy, etc.) to deepfakes. These kinds of activities result in a significant amount of reciprocal sharing between partner agencies.

[18] Mr. Macdonald and CSIS SITE Representative #1 both agreed that attribution of a cyber threat activity to a foreign state is a major challenge, noting that CSE's latest update on

Cyber Threats to Canada's Democratic Process revealed that the source of the majority of cyber threat activity is unattributed, despite best efforts. Mr. Macdonald echoed Ms. Wettlaufer's comments about low barriers to entry, and the complexity of this work. He noted that the agencies have different tools to assess attribution, such as foreign intelligence, which can determine where something started, despite being a difficult exercise. But he also noted that attribution is one tool in assessing the authenticity of online content and that attribution is not always necessary to determine that something is fake and should be publicly identified as such.

[19] In response to a question about how Canada keeps up with these developments, Mr. Macdonald explained that Canada is fortunately not alone in being worried about the rise of generative-AI, and spoke about the "power of community" (academia, media, research institutions, etc.). The intelligence community engages in extensive cooperation with the Five Eyes and our other closest allies, as many of our partners are working on the same issues. Individual departments reach out and have conversations with their international counterparts. Also, SITE reaches out as a task force to similar groups that exist to exchange best practices.

[20] Mr. Macdonald discussed the work of CSE relating to deepfakes and the advancement of this technology. Ms. Wettlaufer noted that RRM Canada's ethical and methodological framework requires that it rely solely on open-source tools. In terms of generative-AI detection, there is no reliable commercially available tool, which is a challenge for RRM Canada. In the past, RRM Canada relied on their SITE partners when they thought something was generative-AI but they were not certain. They have also consulted the Microsoft Threat Assessment Centre. Mr. O'Hayon explained that the RCMP does not have a national security mandate in this respect, where the matter is not tied to a law enforcement issue, but is staying on top of new cyber techniques used by threat actors to conduct FI by collaborating, through its technical staff, with CSIS and CSE or with the Five Eyes or other policing partners. He noted that, with respect to generative AI, the RCMP is seeing its increased use in ordinary criminal activity, like fraud. He also highlighted the increasingly blurred line, especially in the cyber realm, between what is

criminal and what is state-sponsored. A cyber attack might first appear to be linked to criminal activity but actually be directed by a state-sponsored proxy.

[21] Commission Counsel then referred the witnesses to the section of the SITE threat assessment from February 2024[4] addressing cyber threat activity, including the PRC using email operations to target the personal data and work accounts of, among others, Government of Canada officials, politicians, Members of Parliament and ministers. In particular, Commission Counsel asked the witnesses to comment on the following statement in the threat assessment: "[…] *SITE cannot discount the possibility that similar tactics could be used during an election cycle in order to gather intelligence on campaign strategies, fundraising efforts, or possibly policy stances* […]" Mr. Macdonald testified that the PRC is quite active in cyber espionage. Although espionage is not necessarily FI, if threat actors were to engage in espionage and choose to use the resulting information in particular ways (*e.g.*, "hack and leak" operations), then it could potentially impact an election.

[22] CSIS SITE Representative #1 discussed the concept of "pre-positioning" [meaning gaining access to systems or information, not for immediate use, but potentially to be used for future FI activities].

[23] Commission Counsel then referred the witnesses to the section of the SITE threat assessment of February 2024 entitled "Exploiting loopholes in political party nomination processes" and another document that included an update from SITE on specific intelligence.[5] The witnesses were asked if they had seen any other instances of interference or potential interference in nomination processes. CSIS SITE Representative #1 stated that intelligence collection continues. CSIS SITE Representative #1 suggested that foreign states will be more invested in particular ridings during general elections.

[24] In response to a specific question, CSIS SITE Representative #1 explained that they would not choose the word "loophole" to describe the phenomenon of FI in nomination

[4] CAN037690
[5] CAN044584.

contests. Rather, they preferred the language of “vulnerabilities” and “opportunities”. CSIS SITE Representative #1 testified that vulnerabilities in nomination contests are related to political parties’ internal processes and are less a matter within the control of the federal government. Moreover, as nomination races typically take place outside of federal election periods, foreign interference activities may be less likely to be observed. That said, SITE TF’s efforts to develop awareness within the political parties through briefings are ongoing.

[25] Commission Counsel then referred the witnesses to the section of the SITE threat assessment of February 2024 titled, “Money and financing operations,” which describes how threat actors may channel monetary donations or other material support to preferred candidates with the intention of fostering a sense of obligation that can later be leveraged to the foreign-state’s benefit. Counsel noted that recipients were not always aware of the source of donations, so asked for clarification about how a sense of obligation would exist in such cases. CSIS SITE Representative #1 commented that in order for this to create an opportunity for leverage, the candidate would need to be aware that the donation comes from a foreign state. CSIS SITE Representative #1 agreed with the Commission that in a large number of cases, it is not clear if the recipient is aware of the source of the donations and there are a number of intermediaries involved. CSIS SITE Representative #1 added that, in some cases, hostile states, particularly the PRC, can gain leverage or control on an individual through pressure on someone’s personal life or their family living abroad as a possible form of transnational repression. CSIS SITE Representative #1 also agreed with the Commissioner that a foreign state might finance a political candidate's campaign simply because of their perceived favourable views without having the intent to exert influence over the candidate. CSIS SITE Representative #1 further added that the candidate may not even be aware.

[26] Commission Counsel then referred the witnesses to the section of the SITE threat assessment from February 2024 entitled “Mobilizing and leveraging community organizations”. CSIS SITE Representative #1 explained how this constitutes threat

activity and described which country/countries are most likely to engage in this type of activity, and which countries do not.

[27] Commission Counsel asked the witnesses about a statement in the SITE threat assessment from February 2024 CSIS SITE Representative #1 agreed that this is consistent with the broader assessment of the PRC as pragmatic and party agnostic, meaning that PRC officials are flexible and will seek to influence whichever party they believe will win an election. They also consider the policies being advanced by the parties.

[28] Responding to a question about SITE's concerns over PRC interference in provincial, territorial, municipal, and Indigenous election processes, rather than in federal democratic processes and institutions, CSIS SITE Representative #1 testified that with the passing of Bill C-70, CSIS will be in a better position to share intelligence on FI with subnational level governments.

[29] CSIS SITE Representative #1 testified that it is too early to draw conclusions as to how China will position itself in terms of electoral interference in Canada in the next federal election. During the Toronto-St. Paul's by-election, SITE was on the lookout for mis- and disinformation activities from the PRC. The Task Force will keep actively observing this issue. Ms. Wettlaufer noted that RRM Canada saw a spike in reporting on the by-election by publications that have previously engaged in misinformation. However, the reporting observed was neutral. Although they have historically engaged in information manipulation, the publications took no position on the by-election.

[30] In response to a question from the Commission about SITE's mandate and its capacity to look at a broader threat landscape, CSIS SITE Representative #1 noted that the capacity of SITE and the capacity of the different agencies that form part of SITE are two different things. CSIS SITE Representative #1 explained that CSIS has a clear mandate: it collects intelligence with respect to foreign interference, whether it is conducted at the federal or sub-national levels. While monitoring FI activities at the provincial, territorial, municipal, and Indigenous levels is not technically part of the SITE TF mandate, SITE threat assessments nevertheless include reporting on FI in provinces, territories, and other sub-national governments and democratic processes

because it serves as an indicator of what could happen at the national level. This reporting also assists in understanding the general threat environment. CSIS SITE Representative #1 noted that the reporting on sub-national FI activities comes mainly from CSIS, because 1) CSE's mandate is to collect foreign intelligence and 2) RRM Canada's mandate is to monitor the international online space. CSIS SITE Representative #1 opined that a specific agency tasked with monitoring the domestic online space would help to better position ourselves for the future.

[31] Ms. Wettlaufer added that because RRM Canada does not monitor the domestic space on an ongoing basis, every time they are activated for a by-election, there is an opportunity cost for their international work. RRM Canada's team is operating at its maximum capacity. Therefore, some aspect of their international work has to be dropped, paused, postponed or reduced when they receive a new tasking related to the domestic information space for a by-election.

[32] Mr. Macdonald also echoed the distinction between the work done by the SITE TF agencies and the work of the Task Force. CCCS looks at Federal, provincial and municipal elections and reports on all of them where they have information, but SITE itself is focused on Federal elections and it would be difficult to track all elections given their setup and resources.

1.2 Distribution of Sensitive Intelligence

[33] CSIS SITE Representative #2 explained that within CSIS there are guidelines in terms of what types of information might be considered particularly sensitive and therefore require a named distribution list. CSIS SITE Representative #2 confirmed, however, that any intelligence of significance or concern would be raised through CSIS's chain of approval for a decision on further dissemination, including to the Minister.

1.3 The 2023 and 2024 By-Elections

[34] Commission Counsel referred the witnesses to **CAN031449**, a document entitled *Security and Intelligence Threats Task Force and the 19 June 2023 Federal By-Elections*. CSIS SITE Representative #2 indicated that this document was developed by

the **Privy Council Office ("PCO")**, outlining the expectations of SITE with respect to monitoring and assessing FI threats during the June 2023 by-elections. CSIS SITE Representative #2 believes its content accurately captured the scope of SITE TF's work. As set out in the document, SITE produced daily situation reports **("SITREPs")**, held daily touchpoints in order to create those daily SITREPs (all the agencies reported via email or phone whether they had information to add), and SITE met weekly. SITE regularly briefed the Deputy Minister Committee for Intelligence Response ("**DMCIR**") and the DG/ADM Election Security Coordinating Committee ("**DG/ADM ESCC**") on the activities the SITE TF was undertaking and on any intelligence they possessed related to the by-elections. SITE produced both a classified and unclassified report following the vote.

[35] CSIS SITE representative #2 spoke of the baseline threat assessment for the June 2023 by-elections[6] and the baseline threat assessment prior to the July 24, 2023 by-election in the electoral district of Calgary Heritage.[7] Both assessed the likelihood of FI in relation to the by-elections.

[36] Prior to the March 4, 2024, Durham by-election, CSIS SITE Representative #1 explained that SITE drafted the related baseline threat assessment. It encompassed inputs from all of the SITE agencies. CSIS SITE Representative #1 noted that SITE decided to focus on four key threat actors (China, India, Russia and Pakistan), but otherwise kept the same methodology.

[37] CSIS SITE Representative #1 explained the methodology underlying SITE's conclusions in the baseline threat assessments. The SITE assessment took into consideration: any intelligence from SITE agencies indicating whether or not a foreign state had any intent to interfere in the by-election; the demographics of the riding, including diaspora community presence, and the specific candidates running in a riding. CSIS SITE Representative #1 added SITE has discussed whether these reports can be more actionable, including the possibility of developing a robust methodology to assess

[6] CAN020019.
[7] CAN021563

levels of risk for individual ridings. SITE has engaged with the Integrated Terrorism Assessment Centre ("**ITAC**") to discuss their methodology.

[38] CSIS SITE Representative #1 described possible tools that could allow SITE to prioritize its efforts. Mr. Macdonald observed that SITE members have also discussed the risk of drawing too many inferences from by-elections, as they are singular instances. Generally, there is an intention to impact the overall result of an election. As such, unlike the case of a general election, where a state actor will look at the overall system, there is less impact with a single riding.

[39] CSIS SITE Representative #1 testified that SITE agencies coming together to monitor and assess FI with respect to the by-elections is an added benefit for the Task Force. It brought synergy between members and group cohesion. In response to a question from the Commissioner, he stated that it would have been more difficult to develop coordination across agencies if SITE had been activated only once every four years. Mr. O'Hayon added that the fact that SITE TF has been stood up for the by-elections has prompted internal reflection within the RCMP about how to best prepare and organize for the next general election.

[40] In terms of the distribution of its reports during the by-elections, CSIS SITE Representative #2 explained that in the lead up to the June 2023 by-elections, there were concerns about the dissemination of sensitive information following media leaks. As a result, all SITE products are now disseminated and tracked through a new classified system. CSIS SITE representative #1 noted that clients can give feedback on the product via the new system, which he finds very informative. CSIS SITE representative #2 and Mr. Macdonald added that senior clients generally continue to be mostly served by Clients Relations Officers ("**CROs**"), who then track readership of the intelligence and related feedback through the system on the senior clients' behalf.

[41] CSIS SITE Representative #2 explained that SITE reported to DMCIR during the by-elections rather than the Panel of Five, who would be in place during a general election, because the Caretaker convention did not apply and Ministers retained their responsibilities and accountabilities. Therefore, Deputy Ministers would speak to their Ministers if they felt information action needed to be taken in response to information.

Although CSIS SITE Representative #2 was not a member of SITE during a general election, so had never reported to the Panel of Five, it was CSIS SITE Representative #2's understanding that SITE would have reported similar types of information to DMCIR as it would have to the Panel.

[42] The witnesses testified that monitoring the by-elections had resource implications for SITE agencies and for the SITE TF itself.

[43] CSIS SITE Representative #2 explained that, during the by-elections, nearly 100% of their day was devoted towards SITE-related activities: CSIS SITE Representative #2 had engagements with all the CSIS operational branches who would be reviewing the information and intelligence they received to identify threat activity; they were also overseeing the drafting of SITREPs for CSIS and the SITE TF; they had daily check-ins with the SITE members; they were participating in SITE's weekly meeting and briefings to DMCIR; and they had to prepare for briefings to the political parties and others.

[44] Mr. Macdonald estimated that about 10% of his day was focused on outreach out to his teams at CSE for input and then sharing the information with CSIS, in addition to what he already did as part of his regular responsibilities. He confirmed that CSE's threshold for sharing information with the SITE TF during a by-election was the same as it would be during a general election.

[45] Ms. Wettlaufer indicated that about 10% of her day was also spent on SITE activities during by-elections. However, for her team, the impact was much greater. RRM Canada is a small team comprising eight data analysts charged with covering the worldwide online space. Half of the analysts were spending half to two-thirds of their time working on the by-elections. Also, Ms. Wettlaufer indicated that her Deputy Director, in particular, was spending a very significant portion of his time working on the by-elections. Ms. Wettlaufer added that as the chair of the G7 RRM, she should have been traveling and doing much more outreach and coordination with G7 partners. However, she did not do so during by-elections because she felt that she needed to stay close to home and to her team in case there were incidents that arose. Next year, Canada is presiding over the G7 and Ms. Wettlaufer is apprehensive of how to do the required

outreach to deliver on flagship initiatives while also being able to monitor any by-elections or a general election.

[46] Mr. O'Hayon indicated that he also spent about 10% of his time on SITE. However, he noted that there was a greater impact on the Ideologically Motivated Criminal Intelligence Team ("**IMCIT**"). IMCIT is a small team comprising eight people that focuses on monitoring pre-violent extremism. About half of their time was repurposed to look at the by-elections because they do online monitoring and engage with other parts of the RCMP (like the protective service and national security programs). He noted that by-elections are useful because it lets him calibrate what resources will be needed during a general election as he is concerned about burnout and over-burdening the analysts on such a small team, and it allows him to start the process of adding more staff, if needed. Mr. O'Hayon indicated that the RCMP's threshold to share information with the SITE TF during a by-election was the same as during a general election (if he saw something, he would report it).

[47] CSIS SITE Representative #1 added that what has been asked of the SITE TF have been growing over the past year. Although he spent less than 100% of his time on SITE during the Durham by-election, as CSIS SITE Representative #2 had created a solid foundation as prior chair. Now that they are regularly briefing the Panel of Five and providing threat landscape updates, it has again become a full time job for the Chair during a by-election.

[48] Commission Counsel then referred the witnesses to the public version of the SITE TF After Action Report ("**AAR**") in relation to the June 2023 by-elections. CSIS SITE Representative #2 explained that PCO requested that the SITE TF produce a public AAR following the by-elections. CSIS SITE Representative #2 testified that it can be very challenging to produce such a report, or even the public statement that no incidents of FI were observed could reveal intelligence gaps to hostile state actors. In their classified AAR, SITE writes the classification level next to each paragraphs, which facilitates the production of the public AAR. The SITE TF consulted CSIS and the other agencies to ensure that that the release of any particular piece of information would not be detrimental [to critical interests of Canada or its allies, defence or national security].

In the case of the June 2023 by-elections, because the SITE TF did not observe any indications of FI, CSIS SITE Representative #2 noted that it was somewhat simpler to write a public AAR. However, if there is a future by-election where the SITE TF identifies intelligence of threat-related activity, it will become much more difficult to determine what language could be included in a public report.

[49] Mr. Macdonald noted that SITE TF met with a foreign partner after they produced a public report following a general election. He remembers very specifically discussing with that partner their process for including potential FI-incidents in public reports to inform how SITE might respond to such a situation in a Canadian election. CSIS SITE Representative #1 added that the SITE TF is discussing this issue with its Five Eyes partners, which will materialize at some point. He indicated that it is difficult to definitively say what a future public report would look like, but any threat-related content that could be made public would be the subject of discussions between the SITE TF and PCO.

[50] CSIS SITE Representative #2 explained that SITE recognized, in producing a public report, releasing more information to the public would help build FI-resilience in and around elections. The decision to produce a public report was made at the highest levels, and the ADM and DM levels reviewed both the classified and unclassified reports from SITE before they were finalized. Ultimately, DMCIR's decision was that the information in the unclassified AAR was not injurious.

[51] CSIS SITE Representative #1 added that there is a willingness to engage with civil society and Canadians on foreign interference. The SITE TF shares the responsibility to do so as well, even though there are risks associated with publicly disclosing classified information. As part of its efforts to protect democracy, the SITE TF needs to communicate with Canadians, so they know the Task Force exists and that it is actively working to counter FI. To do so in the best way possible, the SITE TF will engage closely with its international partners on best practices. CSIS SITE Representative #1 opined that preparing an unclassified report for the by-elections was relatively easy compared to the challenge of producing an unclassified report following a general election.

[52] CSIS SITE Representative #1 explained that publishing a public-facing AAR following the next general election will be a completely new task for the SITE TF, one they will need to be thinking about from the start of the election campaign. However, although it will not be easy, they will discuss what is possible to release after the election, looking both at what has to be protected but also how certain intelligence can be made public, such as was done in this Commission's unclassified interim report.

[53] Mr. Macdonald highlighted the complexity involved in producing an unclassified AAR and noted that the production of classified AARs by SITE after GE43 and GE44 was already a complicated process, because all agencies involved had to agree on how to characterize complex content, without even needing to consider what could be made public. For the by-elections, SITE was given 90 days to produce AARs, which was workable given the limited amount of information at issue, but completing a public report within that timeframe for a general election might prove difficult.

[54] Ms. Wettlaufer added that in a general election, the question of thresholds – what level of interference constituted a compromise of the integrity of an election, and warranted going public – would need to be made by the Panel of Five. She noted that, although reports from RRM Canada are not classified because the team relies only on open-source information, that does not mean there are no sensitivities to the information RRM Canada assesses and collects. In determining whether to disclose or publicly attribute the online activities it observes, RRM Canada considers international impacts and whether public disclosure is the best tool to achieve the desired outcome, or whether another approach would be more effective.

[55] Commission Counsel referred the witnesses to CAN021929 and CAN032869, the classified AARs of the June and July 2023 by-elections, and asked about SITE's conclusions.

[56] CSIS SITE Representative #2 clarified that the SITE TF was not charged with assessing the impact of FI, but rather reporting on whether it had observed any indication of FI. CSIS SITE Representative #2's understanding is that SITE member agencies detect and identify FI and report and brief that information to either DMCIR or the Panel of

Five. It is those bodies who are charged with assessing the impact of that information on the integrity of elections and taking appropriate action in response.

[57] CSIS SITE Representative #1 added that the SITE TF AARs are best thought of as "tactical reports" of what was observed (or not) by SITE during the by-elections. They are not to be seen as an evaluation or an assessment product (like the SITE TF baseline threat assessments).

1.4 SITE Going Forward

[58] CSIS SITE Representative #2 explained that, before the June 2023 by-elections, the SITE TF was looking at the recommendations from the AAR from GE44[8] as well as some of the reviews that had been done of SITE. In consultation with PCO, SITE TF updated its terms of reference to add a reference to reporting on violent extremism that might be directed toward elections, to formalize what had been done in GE44.[9] Mr. O'Hayon noted that violent extremism was included in SITE's mandate in recognition of the fact that mis- and disinformation can cause criminal conduct, whether or not that information is targeted directly towards Canada. Although they are not necessarily FI, criminal acts and violent extremism can have a tangible effect on the electoral process. Given the RCMP's personal protection mandate, this is the kind of information that his group researches and that the RCMP provides to SITE.

[59] In reflecting on SITE's mandate going forward, Mr. Macdonald explained that the issues relate to benefits and resources. He noted the view that FI is happening at all times and at all levels, but that there is a cost for SITE to be actively monitoring an event. He noted that this cost is offset by the fact that CSIS and CSE are already constantly monitoring FI activities.

[60] CSIS SITE Representative #1 opined that the question of SITE's future is very interesting. First, CSIS SITE Representative #1 testified that SITE's agencies are already doing very well in monitoring both traditional (human to human) and cyber threats. CSIS SITE Representative #1 underlined that in terms of online monitoring,

[8] CAN002359.
[9] CAN021548

there is currently a gap in monitoring the domestic space outside of election periods. CSIS SITE Representative #1 also noted the other levels of government where FI can occur, namely provinces, territories, municipalities, and other sub-national governments. Although this is not part of SITE's mandate, SITE is aware that threat actors have targeted their democratic processes. Second, in terms of producing analytical products, CSIS SITE Representative #1 discussed the possibility that a permanent SITE may be able to do more robust threat assessments from a national perspective – a national threat cartography – that could take the form of the type of "heat map" discussed earlier. This could potentially be an exceptional tool for decision makers and security agencies. Third, SITE could improve its efforts to share information with the general public. Recent reports analyzing how Canada deals with FI suggests that perhaps more work could be done to inform parliamentarians, public servants, staffers, etc. of the threats posed by FI, and SITE could have a corresponding educational mandate. Fourth, a permanent SITE could benefit from more investment to engage with international partners.

[61] Ms. Wettlaufer added that her experience is that SITE is a highly professional and rewarding body to be a part of, in part because it is small and has a clear mandate, despite some ambiguity in its focus on foreign/domestic activity. A permanent SITE could allow some of the baseline work to be done that would allow the Task Force to identify what normal behaviour is, particularly in the online environment. However, Ms. Wettlaufer expressed concern that an expanded mandate would put pressure on her team, which is already very busy. Further, she observed that it is uncomfortable for a foreign affairs ministry to be monitoring the domestic space. Among the G7, Canada is the only foreign ministry that plays such a role. Asked by Commission Counsel whether the domestic monitoring of the online space could be done by another department or elsewhere, Ms. Wettlaufer answered that this was a question to be asked at the DM level, and that RRM Canada's concerns have been shared at that level. For now, her team continues to fulfill this function during elections to the best of its ability and with the support of other SITE members.

[62] Mr. O'Hayon emphasized that RRM Canada has the subject matter experts needed to accomplish its mandate of monitoring the online domain. To replicate that elsewhere,

whether at the RCMP or at CSIS, would require time and effort. There is also the issue of which agency has the authorities and the right mandate for the task.

[63] Asked about SITE TF's relationship with PCO, CSIS SITE Representative #1 explained that PCO Democratic Institutions ("**PCO-DI**") and PCO Security and Intelligence ("**PCO S&I**") attend the SITE TF's meetings as observers. They get a chance to speak during the round table at the end of the meeting. However, the SITE TF may exclude observers when it has discussions about sensitive intelligence. PCO-DI is also involved in communicating with political parties to connect them with SITE TF. CSIS SITE Representative #1 deferred questions about a possible permanent Chair of the SITE TF to senior officials. CSIS SITE Representative #1 noted that the National Counter-Foreign Interference Coordinator ("**NCFIC**") has been discussed as has PCO. CSIS SITE Representative #1 noted the potential benefits and downsides to the choice of PCO, such as PCO being outside the accountability of the SITE agencies' Ministers, but also its proximity to the political aspect of government. CSIS SITE Representative #1 also shared that ITAC is another model that could be considered for SITE, as it has started to play a small role in briefing parliamentarians, is inter-departmental and provides threat assessments.

1.5 The Oxford Riding Nomination

[64] Commission Counsel referred the witnesses, a CSIS 2023 Federal By-Election SITREP [this was a SITREP from CSIS that informed the entry on the SITE TF SITREP], referring to open source allegations of irregularities in the nomination race for the Oxford, Ontario riding.

[65] CSIS SITE Representative #2 testified that CSIS assessed that there was no indication of FI in that case.

2. Examination by the AGC

[66] The AGC asked the witnesses to provide details on the political parties' briefings during the by-elections.

[67] CSIS SITE Representative #2 explained that there was a political party briefing at the unclassified level for the June 2023 by-elections. The briefing was done first in English and then a separate session in French. CSIS SITE Representative #2 believed the New Democratic Party ("**NDP**") and the Bloc Quebecois attended the briefings. Mr. O'Hayon recalled there was at least one other political party present virtually during part of the English briefing but did not remember which one. CSIS SITE Representative #2 noted that no briefing was provided for the July 2023 by-election because it followed the June 2023 by-elections so closely.

[68] The AGC then directed the witnesses to CAN044590, a document dated May 29, 2023 and entitled *SITE TF Briefing to Unclassified Political Parties*. CSIS SITE Representative #2 explained for this political party briefing, the entire SITE Panel was present. This document represents only CSIS SITE Representative #2's speaking points which CSIS SITE Representative #2 read nearly verbatim. This document was translated into French. CSIS SITE Representative #2 also delivered the French presentation and read CSIS SITE Representative #2's speaking points verbatim. CSIS SITE Representative #2 clarified that CSE spoke more specifically and directly to cyber attacks and GAC spoke about disinformation. As a result, CSIS SITE Representative #2 may not have gone into as much detail as contained in CSIS SITE Representative #2's speaking points in regards to these topics, because CSIS SITE Representative #2's colleagues spoke at more length about those issues.

[69] Mr. O'Hayon noted differences between the French and the English briefings prior to the June 2023 by-elections. In his opinion, the English briefing, which was presented first, seemed to miss the mark; SITE did not get questions and the briefing did not appear to sufficiently address the more subtle types of behaviour that constitute FI. Thus, in the French briefing, he added some examples, such as a stolen laptop at a constituency office or volunteers in a campaign you do not recognize, to be illustrative of the kind of more subtle things that can be FI. Mr. O'Hayon felt that, since 2023, the examples have been more tangible and the briefings have become increasingly refined. At the time, however, they did not know what level of understanding the political parties had with respect to FI.

[70] The AGC then directed the witnesses to CAN044589, an email entitled *SITE Unclass Political Party Briefing Feedback*. In response to a question from the AGC, CSIS SITE Representative #2 explained that, in this email, CSIS SITE Representative #2 is reporting on the briefing to two of CSIS' executive officers. CSIS SITE Representative #2 indicated that it was PCO's view that there was a lack of concrete examples in relation to actual FI and that the briefing did not meet the political parties' expectations, and not the view of the attendees, and was provided between the English and French sessions. At the following SITE TF meeting, the members discussed the need to find concrete examples of FI that had perhaps been witnessed in Canada.

[71] CSIS SITE Representative #1 explained that an offer was made to brief the political parties ahead of the March 2024 Durham by-election and the recent Toronto-St. Paul by-election. Both briefings were unclassified, and only attended by the NDP. The SITE TF updated the briefing content based on the feedback it received in 2023. Notably, efforts were made in the briefing for to the Durham by-election to improve the threat assessment by threat country and to ensure there were concrete, open source examples of FI to the briefing. For the Toronto St. Paul by-election briefing, the Task Force further updated the content of the briefing and added further concrete examples of FI, this time based on domestic cases of FI publicly released by this Commission in its Interim Report. SITE also added specific examples of online campaigns that had occurred in Canada, as well as information regarding a follow-up item.

[72] Answering a question from the Commissioner, CSIS SITE Representative #1 said they had no insight into why not all political parties are attending the briefings. CSIS SITE Representative #1 suggested that some political parties might have less interest in them. He added that ahead of the Toronto-St. Paul by-election, general FI briefings were provided to each caucus by the NCFIC, which may have been seen as sufficient. In terms of feedback, CSIS SITE Representative #1 said that he had asked PCO for the parties' feedback and the only thing CSIS SITE Representative #1 was told was that the attendees expressed that concrete cases are better for understanding FI and making it more "real". CSIS SITE representative #1 noted that with the passing of Bill C-70, SITE will be able to leverage new CSIS authorities to share information, especially classified

information, outside of the federal government, including at the subnational level. That said, CSIS has to first determine the procedures for doing so – this is currently underway.

[73] Ms. Wettlaufer indicated that in the case of the disinformation campaign targeting Michael Chong, which RRM Canada tracked on WeChat, the RRM offered to brief Mr. Chong before going public. The GAC Associate Deputy Minister ("**DMA**") did brief Michael Chong. In the case of SPAMOUFLAGE, a PRC-led mis- and disinformation campaign directed against Members of Parliament ("**MPs**"), RRM Canada offered to brief all targeted parliamentarians (47), but in that case only the Conservative caucus asked for a briefing. Ms. Wettlaufer briefed members of the Conservative caucus. Ms. Denham briefed the Chinese dissident who was also targeted.